



Isaca

Isaca-CCOA Exam

ISACA Certified Cybersecurity Operations Analyst

Exam Latest Version: 6.0

DEMO Version

Full Version Features:

- 90 Days Free Updates
- 30 Days Money Back Guarantee
- Instant Download Once Purchased
- 24 Hours Live Chat Support

Full version is available at link below with affordable price.

<https://www.directcertify.com/isaca/isaca-ccoa>

Question 1. (Single Select)

Which of the following is a PRIMARY risk that can be introduced through the use of a site-to-site virtual private network (VPN) with a service provider?

- A: Loss of data integrity
- B: Gaps in visibility to user behavior
- C: Data exfiltration
- D: Denial of service (DoS) attacks

Correct Answer: B

Explanation:

Site-to-site VPNs establish secure, encrypted connections between two networks over the internet, typically used to link corporate networks with remote sites or a service provider's network. However, while these VPNs secure data transmission, they introduce specific risks.

The primary risk associated with a site-to-site VPN with a service provider is the loss of visibility into user behavior. Here's why:

Limited Monitoring: Since the traffic is encrypted and routed through the VPN tunnel, the organization may lose visibility over user activities within the service provider's network.

Blind Spots in Traffic Analysis: Security monitoring tools (like IDS/IPS) that rely on inspecting unencrypted data may be ineffective once data enters the VPN tunnel.

User Behavior Analytics (UBA) Issues: It becomes challenging to track insider threats or compromised accounts due to the encapsulation and encryption of network traffic.

Other options analysis:

A . Loss of data integrity: VPNs generally ensure data integrity using protocols like IPsec, which validates packet integrity.

C . Data exfiltration: While data exfiltration can occur, it is typically a consequence of compromised credentials or insider threats, not a direct result of VPN usage.

D . Denial of service (DoS) attacks: While VPN endpoints can be targeted in a DoS attack, it is

not the primary risk specific to VPN use with a service provider.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 4: Network Security Operations: Discusses risks related to VPNs, including reduced visibility.

Chapter 7: Security Monitoring and Incident Detection: Highlights the importance of maintaining visibility even when using encrypted connections.

Chapter 8: Incident Response and Recovery: Addresses challenges related to VPN monitoring during incidents.

Question 2. (Single Select)

An organization was breached via a web application attack to a database in which user inputs were not validated. This can BEST be described as which type of attack?

- A: Broken access control
- B: Infection
- C: Buffer overflow
- D: X-Path

Correct Answer: A

Explanation:

The described scenario indicates a Injection (i) attack, where the attacker exploits insufficient input validation in a web application to manipulate queries. This type of attack falls under the category of Broken Access Control because:

Improper Input Handling: The application fails to properly sanitize or validate user inputs, allowing malicious commands to execute.

Direct Database Manipulation: Attackers can bypass normal authentication or gain elevated access by injecting code.

OWASP Top Ten 2021: Lists Broken Access Control as a critical risk, often leading to data

breaches when input validation is weak.

Other options analysis:

B . Infection: Typically involves malware, which is not relevant here.

C . Buffer overflow: Involves memory management errors, not manipulation.

D . X-Path: Involves XML query manipulation, not databases.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 4: Web Application Security: Discusses Injection as a common form of broken access control.

Chapter 9: Secure Coding and Development: Stresses the importance of input validation to prevent i.

Question 3. (Single Select)

Which of the following is a KEY difference between traditional deployment methods and continuous integration/continuous deployment (CI/CD)?

- A: CI/CD decreases the frequency of updates.
- B: CI/CD decreases the amount of testing.
- C: CI/CD increases the number of errors.
- D: CI/CD Increases the speed of feedback.

Correct Answer: D

Explanation:

The key difference between traditional deployment methods and CI/CD (Continuous Integration/Continuous Deployment) is the speed and frequency of feedback during the software development lifecycle.

Traditional Deployment: Typically follows a linear, staged approach (e.g., development, testing, production deployment), often resulting in slower feedback loops.

CI/CD Pipelines: Integrate automated testing and deployment processes, allowing developers to quickly identify and resolve issues.

Speed of Feedback: CI/CD tools automatically test code changes upon each commit, providing near-instant feedback. This drastically reduces the time between code changes and error detection.

Rapid Iteration: Teams can immediately address issues, making the development process more efficient and resilient.

Other options analysis:

A . CI/CD decreases the frequency of updates: CI/CD actually increases the frequency of updates by automating the deployment process.

B . CI/CD decreases the amount of testing: CI/CD usually increases testing by integrating automated tests throughout the pipeline.

C . CI/CD increases the number of errors: Proper CI/CD practices reduce errors by catching them early.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 10: Secure DevOps and CI/CD Practices: Discusses how CI/CD improves feedback and rapid bug fixing.

Chapter 7: Automation in Security Operations: Highlights the benefits of automated testing in CI/CD environments.

Question 4. (Single Select)

Exposing the session identifier in a URL is an example of which web application-specific risk?

- A: Cryptographic failures
- B: Insecure design and implementation
- C: Identification and authentication failures
- D: Broken access control

Correct Answer: C

Explanation:

Exposing the session identifier in a URL is a classic example of an identification and authentication failure because:

Session Hijacking Risk: Attackers can intercept session IDs when exposed in URLs, especially through techniques like referrer header leaks or logs.

Session Fixation: If the session ID is predictable or accessible, attackers can force a user to log in with a known ID.

OWASP Top Ten 2021 - Identification and Authentication Failures (A07): Exposing session identifiers makes it easier for attackers to impersonate users.

Secure Implementation: Best practices dictate storing session IDs in HTTP-only cookies rather than in URLs to prevent exposure.

Other options analysis:

A . Cryptographic failures: This risk involves improper encryption practices, not session management.

B . Insecure design and implementation: Broad category, but this specific flaw is more aligned with authentication issues.

D . Broken access control: Involves authorization flaws rather than authentication or session handling.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 4: Web Application Security: Covers session management best practices and related vulnerabilities.

Chapter 8: Application Security Testing: Discusses testing for session-related flaws.

Question 5. (Single Select)

Cyber threat intelligence is MOST important for:

- A: performing root cause analysis for cyber attacks.
- B: configuring SIEM systems and endpoints.
- C: recommending best practices for database security.
- D: revealing adversarial tactics, techniques, and procedures.

Correct Answer: D

Explanation:

Cyber Threat Intelligence (CTI) is primarily focused on understanding the tactics, techniques, and procedures (TTPs) used by adversaries. The goal is to gain insights into:

Attack Patterns: How cybercriminals or threat actors operate.

Indicators of Compromise (IOCs): Data related to attacks, such as IP addresses or domain names.

Threat Actor Profiles: Understanding motives and methods.

Operational Threat Hunting: Using intelligence to proactively search for threats in an environment.

Decision Support: Assisting SOC teams and management in making informed security decisions.

Other options analysis:

A . Performing root cause analysis for cyber attacks: While CTI can inform such analysis, it is not the primary purpose.

B . Configuring SIEM systems and endpoints: CTI can support configuration, but that is not its main function.

C . Recommending best practices for database security: CTI is more focused on threat analysis rather than specific security configurations.

CCOA Official Review Manual, 1st Edition Reference:

Chapter 6: Threat Intelligence and Analysis: Explains how CTI is used to reveal adversarial TTPs.

Chapter 9: Threat Intelligence in Incident Response: Highlights how CTI helps identify emerging

threats.



Full version is available at link below with affordable price.

<https://www.directcertify.com/isaca/isaca-cco>

30% Discount Coupon Code: LimitedTime2025

This advertisement for DirectCertify's Certification Exams Study Guides features a dark background with yellow and white text. A large yellow arrow points from the left towards the main title. On the left, a man in a light blue shirt is shown in a thoughtful pose. A red "PDF" icon and a "FREE TRIAL" badge are also present. The main title "CERTIFICATION EXAMS STUDY GUIDES" is in large, bold, yellow letters, preceded by a yellow asterisk and the text "100% MONEY BACK GUARANTEED". Below this, a list of product features is provided, each preceded by a yellow asterisk. On the right, a hand holding a fan of US dollar bills is shown, along with a badge stating "50K Plus Satisfied Customers". Three circular inset images show people in professional settings. At the bottom right, logos for Visa, American Express, Discover, and Google Pay are displayed. The bottom of the ad features the text "Free Demo for Practice Test & PDF" in white and red.

*** 100% MONEY BACK GUARANTEED**

CERTIFICATION EXAMS STUDY GUIDES

50K Plus Satisfied Customers

*** Product Features**

- * 100% Success in the Final Exam
- * 90 Days Free Updates
- * Latest Exam Q/A
- * 24/7 Customer Support
- * Practice Exams

*** Free Demo for Practice Test & PDF**

VISA AMERICAN EXPRESS DISCOVER G Pay